Appendix J

Windows NT 4.0 Test Report

Topic: AUDIT

Subtopic: Configuration

Test Objective 14 Ensure the audit subsystem is enabled.

DII COE SRS Requirement: None Identified

Rationale: Operating systems generally maintain a number of log files that keep track of system, security, and application information. These log files form the basis of an operating system's auditing subsystem. Auditing can be enabled or disabled. It should always be enabled for a secure system.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Audit from the menu.	The Audit These Events radio button is selected and some events flags are checked off.	Auditing provides accountability. This setting is prerequisite to auditing of specific events.	

Topic: AUDIT

Subtopic: Configuration

Test Objective 15 Ensure audit is correctly configured and collects the required audit events (login and logout, use of privileged commands, application and session initiation, use of print command, DAC permission modification, export to media...).

DII COE SRS Requirement: 3.2.2.5 At a minimum, the following audit events shall be audited:
3.2.2.5.1 Login (unsuccessful and successful) and Logout (successful)
3.2.2.5.2 Use of privileged commands (unsuccessful and successful)
3.2.2.5.3 Application and session initiation (unsuccessful and successful)
3.2.2.5.4 Use of print command (unsuccessful and successful)
3.2.2.5.5 Discretionary access control permission modification (unsuccessful and successful)
3.2.2.5.6 Export to media (successful)
3.2.2.5.7 Unauthorized access attempts to files (unsuccessful)
3.2.2.5.8 System startup and shutdown (unsuccessful and successful).

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Audit from the menu.	The Audit These Events radio button is selected. The Use of User Rights Failure checkbox is checked. The Security Policy Changes Success and Failure checkboxes are checked. The Restart, Shutdown, and System Success and Failure checkboxes are checked.	Auditing provides accountability. This setting is prerequisite to auditing of specific events.	
2	In the Taskbar, choose Start, Programs then Explorer. When the Exploring window appears, select the root directory, such as "C:", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Auditing.	Replace Auditing on Subdirectories is checked off. Replace Auditing on Existing Files is checked off. The group "Everyone" is displayed in the "Name" listbox. The "Change Permissions" Success and Failure checkboxes are checked for the group "Everyone". The "Take Ownership" Success and Failure checkboxes are checked for the group "Everyone". The "Write" and "Delete" Success checkbox is checked for the group "Everyone" for critical directories and files, including the system files referenced earlier, other system files, application files, and user files as determined by the site administrator.		

3	Verify that significant changes to selected Registry keys are audited. Use the Registry Editor (regedt32.exe) - the Registry Editor can be located using the Explorer and selecting the "C:\WINNT\system32" directory, then launching the "regedt32.exe" program by double clicking on it. When the Registry editor window appears, select HKEY_LOCAL_MACHINE\Software\ Program Groups window, then select the "Security", and "Auditing" menu choices.	Significant changes are audited.		

Topic: AUDIT

Subtopic: Audit of Unsuccessful login attempts

Test Objective 273 Verify that unsuccessful login attempts are logged.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Audit from the menu.	In the Audit Policy window, the Audit These Events radio button is selected. The Logon and Logoff Failure checkbox is checked.		

Topic: AUDIT

Subtopic:

Test Objective 196 Verify the system is capable of detecting when the audit file reaches a configurable threshold and audit records are not lost if this threshold is reached. If the audit file becomes full, verify the system is shutdown until the audit data is archived.

DII COE SRS Requirement: 3.2.2.1.3 The COE shall be capable of detecting when the audit trail reaches a configurable threshold (i.e., % of capacity), ensuring that audit data is not lost, and maintaining system availability.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then select Event Viewer. Select "Log", "Security" from the menu. Select "Log", "Log Settings ... " from the menu. In the "Event Log Settings" window, verify the "Maximum Log Size" entry.	The "Maximum Log Size" entry is set to at least 2 MB.	To ensure that system availability is maintained, verify that the security (audit) log is directed to a large, reliable storage device.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then select Event Viewer. Select "Log", "Security" from the menu. Select "Log", "Log Settings ... " from the menu. In the "Event Log Settings" window, verify that "Do Not Overwrite Events (Clear Log Manually)" is selected.	The "Event Log Wrapping" choice "Do Not Overwrite Events (Clear Log Manually)" is selected.		

Topic: AUDIT

Subtopic: Archival of Audit Data

Test Objective 27 Verify the system provides a configurable capability to archive audit data.

DII COE SRS Requirement: 3.2.2.1.4 The COE shall provide a configurable capability to archive audit data.

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then select Event Viewer. Select "Log", "Security" from the menu. Select "Log" from the menu. Select the "Save As ... " choice from the "Log" menu item.	The Save As dialog box appears allowing the saving of the log to an administrator selected location.	The audit log can get full; regular backups of the audit trail will avoid shutdown of the system.	

Topic: AUDIT

Subtopic: Audit Reduction

Test Objective 24 Determine if an audit reduction capability exists. This capability can be either OS provided or an add-on product.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Interview the System Administrator to determine if audit data is reviewed and if so, if an audit reduction utility is used.	Audit data is reviewed and an audit reduction tool is utilized to aid in the review.	The native Windows NT audit reduction capability does not provide the best possible analysis of large audit logs. A utility such as DumpEvt can be used to dump the event logs (audit files). DumpEvt can be obtained from "http://www.somarsoft.com".	

Topic: AUDIT

Subtopic: Configuration

Test Objective 197 Verify required audit events are recorded in the audit log (login and logout, use of privileged commands, application and session initiation, use of print command, DAC modification, export to media, unauthorized access attempts to files . . .).

DII COE SRS Requirement: 3.2.2.5 At a minimum, the following audit events shall be audited:
3.2.2.5.1 Login (unsuccessful and successful) and Logout (successful)
3.2.2.5.2 Use of privileged commands (unsuccessful and successful)
3.2.2.5.3 Application and session initiation (unsuccessful and successful)
3.2.2.5.4 Use of print command (unsuccessful and successful)
3.2.2.5.5 Discretionary access control permission modification (unsuccessful and successful)
3.2.2.5.6 Export to media (successful)
3.2.2.5.7 Unauthorized access attempts to files (unsuccessful)
3.2.2.5.8 System startup and shutdown (unsuccessful and successful).

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then select Event Viewer. Select "Log", "Security" from the menu. Verify that the Security log contains all required events.	The Security log contains all required events.		

Topic: AUDIT

Subtopic: Configuration

Test Objective 25 Verify the audit data is protected by the system so that access to it is limited to only those authorized to view the audit data. In addition, verify the audit data is protected from change or deletion by general users.

DII COE SRS Requirement: 3.2.2.1.1 The audit data shall be protected by the system so that access to it is limited to those who are authorized to view audit data.
3.2.2.1.2 The audit function shall be protected from change or deletion by general users.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32\CONFIG" directory. Then select each of the following files in turn, right click each, chose Properties, click the Security tab, then select the Permissions button: SysEvent.Evt SecEvent.Evt AppEvent.Evt	Each of the files show the following permissions: Administrators - Full Control SYSTEM - Full Control	The audit log should be protected.	
2	Verify that the security (audit) log is maintained on a physically protected system, such as the site's domain controller. Use a third-party audit tool, on a regular basis, to copy the Security log to a physically protected system.	The audit log is maintained on a physically protected system.	The audit log should be protected.	
3	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the form. Select "Generate security audits" from the "Right" dropdown list.	No user or group account is listed in the "Grant to" listbox.	The right to create security audits is protected.	
4	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then	No user or group account is listed in the "Grant to" listbox.	The right to manage auditing and the security log is protected.	

	User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the form. Select "Manage auditing and security log" from the "Right" dropdown list.			

Topic: Availability

Subtopic: Emergency Repair Disk

Test Objective 163 Verify that a current emergency repair disk has been created, updated, and is protected with an appropriate password.

DII COE SRS Requirement: None Identified

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	Verify that a current emergency repair disk is available for each Windows NT system. Interview the System Administrator and check the creation date of the disk. The rdisk utility can be used to create a new emergency repair disk.	The System Administrator creates a current emergency repair disk regularly. The disk is labeled with the system name and the date on the repair disk is less than six months old.	Windows NT uses the emergency repair disk to recover from errors and allows recovery if the system should become so damaged that it cannot be booted. The emergency repair disk provides full access to all system components and data, therefore, it should be protected appropriately.	

Topic: DAC

Subtopic: Access to I/O Devices

Test Objective 60 Verify DAC mechanisms are used to restrict access by general users to input/output (I/O) devices, such as floppy disks and tape drives, and the capability to specify which users may access I/O devices.

DII COE SRS Requirement: 3.2.4.11 The COE shall be capable of using DAC mechanisms to restrict access by general users to input/output (I/O) devices, such as floppy disks and tape drives.
3.2.4.11.1 The COE shall provide a capability to specify which users may access I/O devices.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify that access to floppy disks is restricted to the user currently logged on. In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon".	The "AllocateFloppies" key is set to "1".	By default, "AllocateFloppies" will not be in the registry key. To add "AllocateFloppies" see configuration steps.	
2	In the Exploring window, select the floppy, such as "3_ Floppy (A:)", right click it, then choose Properties. When the Properties window appears, select the Sharing tab, then check off the Not Shared dialog box.	The floppy is not shared over the network.	Remote access to the floppy drive is rarely needed. A process can remain running in the background after the user logs off and then access the floppy drive while another user is logged on.	
3	Verify that access to CD-ROM disks is restricted to the user currently logged on. Run "Regedt32". When the Registry Editor appears, click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT	The "AllocateCDRom" key is set to "1".	This should be done if the system is not intended to be a CD-ROM server. If remote access is enabled the user who inserts a CD-ROM may not be aware	

	\CurrentVersion\Winlogon\AllocateCDRom".		that other users can read it and may insert a CD-ROM that is not intended for general access. In addition, a process can remain running in the background after the user logs off, and access the CD-ROM drive while another user is logged on.	
4	In the Exploring window, select the CD_ROM, such as "(D:)", right click it, then choose Properties. When the Properties window appears, select the Sharing tab, then check off the Not Shared dialog box.	The CD-ROM is not shared over the network.		

Topic: DAC

Subtopic: Deadman Lockout

Test Objective 58 Verify a Deadman Timeout function locks a user's terminal if input devices have been idle for a configurable period of time (default 5 minutes) and that users are required to re-authenticate themselves to unlock a locked terminal.

DII COE SRS Requirement: 3.2.4.12 The COE shall provide a deadman function that locks the user's terminal if user input devices have been idle for longer than a configurable time period.
3.2.4.12.1 The configurable time period shall default to 5 minutes.
3.2.4.12.2 Any user input device may be used to restore a locked terminal.
3.2.4.12.3 The specific input value (whether from keyboard, mouse, or other pointer) used to activate the function that restores the locked terminal shall be ignored except to activate the function.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify that a screen saver is enabled for all accounts by interviewing the System Administrator and determining that either mandatory profiles that enforce use of a password protected screensaver, or a training program to train users to use screensavers with password protection are in use.	Mandatory profiles that enforce use of a password protected screensaver, or a training program to train users to use screensavers with password protection are in use.	Train users NOT to change the screen saver settings that they are given by default. This protects against a user account from being used by an unauthorized person if a user steps away from the system. A mandatory profile can enforce the screensaver security policy as well as other security policies for users. Mandatory profiles are discussed in objective 286.	
2	Verify that new user accounts are set up with screen saver enabled and set to require a password to clear. Set up a new account and verify that the screen saver is enabled.	Screen saver is automatically enabled with the creation of new accounts.	The system should be locked through a password protected screen saver when it is left unattended.	

Topic: DAC

Subtopic: Permissions

Test Objective 53 Verify System Administration Tools are configured securely and their use is limited to appropriate users.

DII COE SRS Requirement: None Identified

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT" directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click the Default User, then System, finally Restrictions.	The entry "Disable Registry editing tools" is checked off.		
2	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT" directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click the Default User, then Windows NT Shell, finally Restrictions.	The entry "Remove common program groups from Start menu" is checked off.	Administration tools appear in common program groups.	

Topic: DAC

Subtopic: DAC TCSEC Requirements

Test Objective 270 Verify that the Operating System was designed to satisfy the C2 level of trust as defined by the TCSEC.

DII COE SRS Requirement: None Identified

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	Run the c2config.exe tool from the Windows NT Resource Kit for NT 4.0. It includes secure configuration for both the system directories and the Registry (ACLs).	The operating system configuration will be closer to C2 certification.	Be on the look out for the latest version of the c2config.exe tool.	

Topic: DAC

Subtopic: Least Privilege

Test Objective 284 Verify that users and groups available on the system have the appropriate privileges.

DII COE SRS Requirement: None Identified

Rationale:

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select "Log on locally" from the "Right" dropdown list and check the groups this right is assigned to. In the "Grant To" box verify that the groups "Everyone" and "Guests" are not listed.	The groups "Everyone" and "Guests" are not listed in the "Grant To" box.	Guest is a member of group Everyone and this is one of several steps that can be taken to limit access to the system via this unsafe login. General users will retain the right to log on locally if the group Users is granted the right.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the form. Select each right one at a time from the "Right" dropdown list and verify the users granted each right.	The rights for the "Users" group have been restricted to the "Log on locally", "Shut down the system", and, if needed for operational reasons, "Access this computer from network" rights.	These are the only rights needed for operational work, and by the principle of least privilege no additional rights should be granted. Depending on the operational use of the system, the right "Access this computer from network" may be needed, but this right should not be granted unless it is specifically required.	
3	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, check off the "Show Advanced Rights" checkbox in the lower left corner of the form. Select the "Debug programs" right from the "Right" dropdown list and view the users granted the right. Verify that no user, not even "Administrator", has the "Debug	No User is listed in the "Grant to" listbox.	This right should NOT be enabled if the system is a production system. Users with the "Debug Programs" right can access system memory where sensitive information, such as passwords, may be cached.	

	programs" right.			
4	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, check off the "Show Advanced Rights" checkbox in the lower left corner of the form. Select the "Log on as a service" right from the "Right" dropdown list and view the users granted the chosen right. Verify that no user, not even Administrator, has the "Log on as a service" right.	No User is listed in the "Grant to" listbox.	This right allows a process to register as a system service. Since services are usually installed using the "Services" control panel, this right is not needed.	
5	Verify that third party services run under an account in which rights have been tailored to include only those rights essential to allow the service to perform its function. In addition, no service should run under the "Administrator" account.			

Topic: DAC

Subtopic: Permissions

Test Objective 257 Verify that permissions on all "temp" directories are set correctly.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the System icon. When the System Properties dialog box appears, select the Environment tab, then find the Temporary directory assignment. In the Exploring window, right click each TEMP/TMP directory listed, then select Properties. When the Properties dialog box appears, select Security tab, then Permissions box.	Permissions on all TEMP directories are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Add permission only SYSTEM - Full Control Users - Add permission only	A TEMP directory is one defined by the current environment variable "TEMP" or "TMP." TEMP directories are used by many applications as a repository for temporary files containing data that should be protected from access by unauthorized users.	

Topic: DAC

Subtopic: Registry Keys

Test Objective 258 Verify that all Registry key ACLs used to support applications have been set correctly.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify that ACLs on all Registry keys used to support applications not needed by "Guest" have been set to deny write and execute access for the group "Everyone", but have granted the "write" and "execute" accesses for the group "Users". NOTE: This should only be done if the group "Everyone" previously had "write" and "execute" access.	The ACLs on all Registry keys used to support applications not needed by "Guest" have been set to deny write and execute access for the group "Everyone", but have granted the "write" and "execute" accesses for the group "Users".	This should be done if some applications depend on the availability of the "Guest" account and the applications cannot be rewritten to not depend on this account. This setting will limit to some degree the damage that can be done if an attacker accesses the system using the "Guest" account. A utility such as "DumpACL" can be used to dump the ACLs for the entire registry. Even using this utility, this task will be labor intensive and require determining which applications do not require the "Guest" account. DumpACL can be obtained from "http://www.somarsoft.com".	

Topic: FILE SYS SEC

Subtopic: IP source routing and IP forwarding

Test Objective 80 Verify that IP forwarding and IP source routing has been disabled.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Network icon. When the Network dialog box appears, select the Protocols tab, then double click on the TCP/IP Protocol entry. In the Microsoft TCP/IP Properties window, click on the Routing tab.	The Enable IP Forwarding item is NOT checked off.		

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 66 Ensure the file systems are configured correctly and securely.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then Disk Administrator. Ensure that the "File Type" for each hard disk listed is NTFS.	The file system type on all hard drives listed is NTFS.	The NTFS file system is the only file system that supports DAC for file system objects.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then Disk Administrator. Select "Partition" from the menu and verify that the "Secure System Partition" option is enabled.	The "Secure System Partition" should be selected. This will restrict access of the FAT boot partition to "Administrators" only and protects the system files on the FAT boot partition.	This should be done if the system is a RISC system.	

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 67 Verify file permissions are set appropriately throughout the file system.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs then Explorer. When the Exploring window appears, select a directory, such as "C:", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the permissions on the directory. Repeat this procedure for other hard disk partitions, such as "D:", "E:", etc.	The permissions on each directory are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Add and Read System Operators - Add and Read System - Full Control These permissions allow the group "Everyone" to create and add new files and directories, and by default, only the creator, "System", or "Administrators" accounts will have access to the newly created files.	These settings provide basic protection for each partition in the system. They also protect system files in the root directory, such as autoexec.bat, from being deleted and replaced with an attacker's version.	
2	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select the "C:\Boot.ini" file, right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the file permissions. Repeat this procedure for files "C:\Ntdetect.com" and "C:\Ntldr".	The file permissions are set to: Administrators - Full Control SYSTEM - Full Control	These settings are specified for C2 configuration for Intel platforms.	
3	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select the "C:\AUTOEXEC.BAT" file, right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the file permissions. Repeat this procedure for file "C:\CONFIG.SYS".	The file permissions are set to: Everyone - Read Administrators - Full Control SYSTEM - Full Control	These settings are specified for C2 configuration on Intel platforms, and protect the operating system from unauthorized modification.	
4	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory	The directory permissions are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read SYSTEM - Full Control Users - Change	These settings protect the operating system from unauthorized modification. Use the settings recommended here, then relax permissions as needed and approved by	

	permissions.	The groups "Everyone" or "Users" do NOT have "Delete" access.	the responsible security officer. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. This is not as restrictive as is desirable, since it gives the "Users" group the "Change access" right to all "*.ini" files although this right may not be needed. Identifying which applications need the "Change access" right to their ".ini" files is difficult to do with complete accuracy. NOTE: The c2config.exe tool from the Windows NT Resource Kit for NT 4.0 includes a secure configuration for the system directories; the DACLs provided by that tool are less restrictive, and therefore, more risky, than those recommended here.	
5	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the permissions on all "*.ini" files.	The permissions are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read SYSTEM - Full Control Users - Change The groups "Everyone" or "Users" do NOT have "Delete" access.	These settings protect the operating system from unauthorized modification. Use the settings recommended here, then relax permissions as needed and approved by the responsible security officer. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. This is not as restrictive as is desirable, since it gives the "Users" group the "Change access" right to all "*.ini" files although this right may not be needed. Identifying	

			which applications need the "Change access" right to their ".ini" files is difficult to do with complete accuracy. NOTE: The c2config.exe tool from the Windows NT Resource Kit for NT 4.0 includes a secure configuration for the system directories; the DACLs provided by that tool are less restrictive, and therefore, more risky, than those recommended here. Some applications and services that are used at a site may require greater access than those recommended here. Each relaxation of permissions should be analyzed to determine its security impact.	
6	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	The permissions are set to: Administrators - Full Control CREATOR OWNERS - Full Control Everyone - Read Server Operators - Change SYSTEM - Full Control The groups "Everyone" or "Users" do NOT have "Delete" access.	These settings are specified for C2 configuration and protect the operating system from unauthorized modification. Relax permissions as needed and approved by the responsible security officer. NOTE: The c2config.exe tool from the Windows NT Resource Kit for NT 4.0 includes a secure configuration for the system directories; the DACLs provided by that tool are less restrictive, and therefore, more risky, than those recommended here. Using these settings, only administrators will be able to install most applications, and users of 16-bit applications may not be able to customize options. If these settings prove too restrictive, users may be given the "Change"	

			permission.	
7	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM32", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	The permissions on this directory are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read Server Operators - Change SYSTEM - Full Control	These settings protect the operating system from unauthorized modification.	
8	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM32\DRIVERS", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	The permissions on this directory are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read Server Operators - Full Control SYSTEM - Full Control	These settings are specified for C2 configuration and protect the operating system from unauthorized modification.	
9	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM32\CONFIG", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	Verify that permissions are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - List SYSTEM - Full Control	NOTE: If these settings are propagated to subdirectories, the groups "Everyone" and "Users" will be able to create a profile, but won't be able to read other users' profiles.	
10	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM32\SPOOL", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	The permissions are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read Print Operators - Full Control Power Users - Change Server Operators - Full Control SYSTEM - Full Control	These settings are specified for C2 configuration.	
11	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\SYSTEM32\". Verify that the "OS2" directory does not exist.	This directory does NOT exist.	OS/2 commands are not needed, and any unnecessary complexity of the operating system potentially increases vulnerability. The OS/2 subsystem is not used in the C2 configuration. NOTE: The POSIX subsystem is also not used in the C2 configuration.	
12	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select the shared	The permissions on the shared directory used as a central repository for user profiles are set to:	Profiles can contain sensitive information. This setting protects	

	directory used as a central repository for user profiles (normally "\<SYSTEMROOT>\WINNT\Profiles), right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	Administrators - Full Control CREATOR OWNER - Full Control SYSTEM - Full Control Everyone - Add	against attacks based on substituting or copying a profile.	

Topic: FILE SYS SEC

Subtopic: System Shutdown

Test Objective 84 Verify if the machine is a server, domain controller, or it’s availability is otherwise critical, it cannot be shutdown without first logging on.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify the system cannot be shut down without logging on. In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon" registry key.	The "HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows NT\ CurrentVersion\Winlogon\ ShutdownWithoutLogon" registry key is set to zero.	Only authorized users should be allowed to shut down critical systems, therefore, this should be done if the machine is a server or domain controller, or it’s availability is otherwise critical. The risk of someone simply pulling the plug is less than the risk of someone shutting down the system from the login prompt screen.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the form. Select "Force shut down from a remote system" from the "Right" dropdown list.	No user or group account is listed in the "Grant to" listbox.	No user or group can shut down the system remotely.	

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 259 Verify that permissions on the "Repair" function are set correctly.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT\REPAIR", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions.	The permissions are set to: Administrators, Full Control	This setting is specified for C2 configuration. Running the repair function may give access to all data on the system, therefore, access to this function should be tightly controlled.	

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 260 Verify that permissions on the backup program are set correctly.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select file "C:\WINNT\SYSTEM32\NTBACKUP. EXE ", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the file permissions.	The file permissions are set to: Administrators - Full Control SYSTEM - Full Control	These settings protect the backup program from unauthorized modification.	

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 261 Verify that file permissions on all executable files are set correctly.

DII COE SRS Requirement: None Identified

Rationale: Trojan horses and many viruses replicate by modifying executable files.

#	Required Action	Expected Results	Comments	Ö
1	Verify that all executable files have read and execute permission but NOT write permission granted to users authorized to execute the program. NOTE: Users specifically authorized to maintain executable files are an exception to this rule. This test objective can be verified by using the program DumpAcl to generate a report on file system permissions. The resulting report can then be filtered with the string ".exe". If any of these executable files are modifiable by the group "Users", go to the File Manager and remove the write permissions on those files for the "Users" group.	The resulting permissions on all executable files should be: CREATOR OWNER - Full Control Everyone - Read System - Full Control Administrators - Full Control		

Topic: FILE SYS SEC

Subtopic: Permissions

Test Objective 262 Verify that permissions on directories containing executable files are set correctly.

DII COE SRS Requirement: None Identified

Rationale: Necessary to protect executable files, including operating system files, from being replaced by versions containing Trojan Horses.

#	Required Action	Expected Results	Comments	Ö
1	Verify that directories containing executable files deny write permission to all users not specifically authorized to maintain the executables contained in the directory. In the Taskbar, choose Start, Programs, then Explorer. When the Exploring window appears, select directory "C:\WINNT ", right click it, then choose Properties. When the Properties window appears, select the Security tab, then Permissions. Verify the directory permissions and then repeat the procedure for the following directory: C:\WINNT\SYSTEM32	The permissions on the subdirectories (NOT the files) are: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read SYSTEM - Full Control NOTE: The boxes "Replace Permissions on Subdirectories" or "Replace Permissions on Existing Files" are NOT checked.	After new software is installed, check that this security recommendation is still being met and take action if necessary. In the Exploring window, search for *.exe, *.bat, and *.com to identify all directories containing executables.	

Topic: FILE SYS SEC

Subtopic: System Shutdown

Test Objective 263 Verify that only privileged users can shutdown, reboot, or restart a system (either locally or remotely).

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify the groups "Everyone" and "Guests" do not have the right to shut down the system: In the "Program Manager" in the "Administrative Tools" group, select the "User Manager" file. Select "Policies", "User Rights" from the menu. Select "Shut down the system" from the "Right" pull down menu and verify that the "Users" group IS listed and the groups "Everyone" and "Guests" are NOT.	The groups "Everyone" and "Guests" are NOT listed for the "Shut down the system" right.	This limits the effects that the built-in "Guest" account can have on the system. General users may still shutdown the system if the "Users" group is granted this right.	
2	If the machine is a server or domain controller, verify that the "Users" group does not have the right to shut down the system. In the "Program Manager" in the "Administrative Tools" group, select the "User Manager" file. Select "Policies", "User Rights" from the menu. Select "Shut down the system" from the "Right" pull down menu and verify that the "Users" group is NOT listed.	The "Users" group is NOT listed for the "Shut down the system" right.	This should be done if the machine is a server or domain controller.	
3	Verify that only "Administrators" and "Power Users" may shut down the system from a remote site: In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the	Only privileged users or groups are listed in the "Grant to" listbox. The "Administrators" and "Power Users" groups should be listed for this right because it protects availability of the system, yet allows remote control for sites that don’t administer their own systems.	Only privileged users can shut down the system.	

	form. Select "Shut down the system" from the "Right" dropdown list.			
4	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT" directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click the Default User, then Shell, finally Restrictions.	Check off Disable Shut Down command.	Restriction of the shut down command.	

Topic: HARDWARE/FIRMWARE

Subtopic: Boot Password

Test Objective 184 Verify the single user boot or system firmware password is set, and the system is configured such that a password must be entered to boot to a single-user state.

DII COE SRS Requirement: 3.2.12.3 The COE shall be configured such that a password must be entered to boot to a single-user state.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify that the system firmware has been configured to require a password to boot the system. Use procedures provided by the BIOS vendor.	A password is required to boot the system.	This should be done if the option of defining which drives are bootable is not available in the system firmware.	
2	Verify that the system firmware can only be accessed by password and supports an option defining which drives are bootable.	A password restricts booting the system into a non-secure operating system while still allowing system boots without password.	If necessary, upgrade the system BIOS chip. This should be done if the option of defining which drives are bootable is not available in the system firmware.	
3	Verify that the system BIOS chip supports a boot password that is required for both cold and warm boot.	The system cannot be booted without a password. Makes it more difficult for attackers to boot the system into a non-secure operating system.	Some system BIOS chips support a boot password that is required for both a cold and warm boot. This option makes it more difficult for attackers to boot the system into a non-secure operating system. If necessary, upgrade the system BIOS chip.	

Topic: Hardware/Firmware

Subtopic: Physical Protection

Test Objective 186 Determine if the proper physical protections are used.

DII COE SRS Requirement: None Identified

Rationale: Access to the domain controller is required for most user activities and becomes a major single point of failure. Domain controllers are a single point of attack for user capabilities. If any account with administrative rights is compromised, the attacker can change rights of any user on network.

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	Verify that critical systems are physically protected so attacker cannot replace BIOS or drain BIOS battery or carry away disk drives.	Systems are physically protected.	Physical access can be used to bypass Windows NT security features.	
2	Verify that removable media is stored in a physically secure location. Train System Administrators and users that data on floppy disks and backup media is NOT protected by file system security.	Backups and floppies are handled securely.	Data on removable media (i.e., backup tapes and floppies) is not protected by Windows NT 4.0 file access controls. A backed up file can be restored to a volume that does not have security enabled, on any system; therefore, backups must be controlled.	

Topic: I&A

Subtopic: Accounts

Test Objective 118 Verify that privileged users have a second user account to use for everyday, operational work.

DII COE SRS Requirement: None Identified

Rationale: Having a second account limits the damage that can be done by software run by a system administrator engaged in non-administrative activities. For example if a privileged user runs software infected by a virus or Trojan horse using their privileged account, the application may be able to bypass operating system protections.

#	Required Action	Expected Results	Comments	Ö
1	Verify that users that are members of "Administrators" and/or Domain Administrators group(s) do not use their accounts for everyday operational work.	All users with accounts that are members of the "Administrators" and/or Domain Administrators group(s) have a second account that is not a member of either group and are trained to use it when not engaged in system administrative work.		

Topic: I&A

Subtopic: Accounts

Test Objective 121 Verify that general user accounts do not have administrator privileges.

DII COE SRS Requirement: None Identified

Rationale: Limits the damage that can be done by operational software. If some users need a subset of Administrator group rights a group with a subset of administrator rights should be created and users are assigned to it. Implements rule of least privilege.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, select the "Show Advanced Rights" checkbox in the lower left corner of the form. Select each user right from the "Right" dropdown list. Review each privilege assigned to the "Users" group.	The Least possible privileges that allow completion of the mission are granted to the "Users" group.	Accounts used for operational work should only be members of the "Users" group and should not have unnecessary rights granted.	

Topic: I&A

Subtopic: Login

Test Objective 108 Verify the system provides the capability to restrict multiple login failures, locks out the userID and prohibits further login if the threshold is reached, sends notification to the appropriate personnel, and allows restoration of the locked out userID.

DII COE SRS Requirement:
3.2.1.7 The COE shall provide a capability to restrict multiple login failures.
3.2.1.7.1 If the number of login failures reaches a configurable threshold (0 through 5), the userID shall be locked and the user shall be prohibited from further login attempts.
3.2.1.7.2 If the number of multiple login failures is set to 0, the capability shall be disabled.
3.2.1.7.3 If a userID is locked, the COE shall send a notification to the appropriate person.
3.2.1.7.4 The COE shall provide the capability to restore locked userIDs.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. Verify that the number of failed logins before lockout is set to five attempts.	In the "Account Policy" dialog box the "Lockout after - bad logon attempts" box should be set to five attempts.	Five attempts is enough for even the sleepiest user to type the password correctly, but is too few for most password-guessing attacks.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. Verify that the time period to reset the failed login attempt counter is set to 30 minutes.	In the "Account Policy" dialog box the "Reset count after - minutes" box is set to 30 minutes.	Limits the effectiveness of password guessing attacks.	
3	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. Verify that the delay before automatically reopening account after lockout is set to forever.	In the "Account Policy" dialog box the "Forever" box in the "Lockout Duration" list box should be checked.	This ensures that System Administrator must intervene and enforces administration awareness of password-guessing attacks.	
4	Modify the domain policies for password complexity and administrator lockout. Install the appropriate Microsoft Resource Kit	Passwords will be complex and the Administrator account can be locked out from network logon.	Increases the protection of the Administrator account and limits the effectiveness of password guessing	

	(server or workstation). Run the following utility at a DOS command prompt: PASSPROP /complex /adminlockout The option "/complex" forces passwords to be complex, requiring passwords to be a mix of upper and lowercase letters and numbers or symbols. The option "/adminlockout" allows the Administrator account to be locked out. The Administrator account can still log on interactively (locally) on domain controllers. NOTE: Additional properties can be set using User Manager or the NET ACCOUNTS command as required.		attacks.	

Topic: I&A

Subtopic: Password Management

Test Objective 105 Verify the system enforces individual user accountability, a globally-unique valid userID and password is required for all users to access the system, and the user's identity is associated with all auditable actions performed.

DII COE SRS Requirement: 3.2.1.1 The COE shall enforce individual accountability by providing the capability to uniquely identify each individual system user.
3.2.1.1.1 The COE shall require users to identify themselves before beginning to perform any actions that the system is expected to mediate.
3.2.1.2 Each user shall be identified by a globally unique user name or userID that will follow a standard set of processes or rules for formation.
3.2.1.3 The COE shall provide the capability of associating the user's identity with all auditable actions taken by that individual.

Rationale: Simply put, accounts without passwords should not be allowed on any system. An account without a password is an easy target for an intruder and subjects the entire system to risk.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, verify that the "Guest" account has not been disabled and has a password.	The Guest account has a strong password making it difficult for intruders to access the system.	This should be done if some applications depend on the availability of "Guest" and cannot be rewritten not to depend on the Guest account. The extra protection is needed because "Guest" is a member of group "Everyone", which has read rights on many Registry keys.	

Topic: I&A

Subtopic: Password Management

Test Objective 111 Verify trivial passwords are not used for accounts.

DII COE SRS Requirement: 3.2.1.4 The COE shall use a protected mechanism (e.g., passwords) to authenticate each user's identity. If passwords are used as the mechanism, they shall meet the following requirements:

3.2.1.4.1 Passwords shall be at least eight alphanumeric characters in length.
3.2.1.4.3 The COE shall provide a graphical user interface (GUI) for selection of passwords.
3.2.1.4.4 The COE shall provide the capability for users, or the system to generate passwords only in accordance with specified selection rules.
3.2.1.4.5 Password selection rules shall be configurable by the site security officer. These rules shall include the following:
3.2.1.4.5.1 Maximum password age
3.2.1.4.5.2 Minimum password age
3.2.1.4.5.3 Password character set (e.g., alphanumeric plus special characters)
3.2.1.4.5.4 Minimum of one numeric character (i.e., 0-9)
3.2.1.4.5.5 Prohibit repeating characters (e.g., ee)
3.2.1.4.5.6 Dictionary words prohibited.

Rationale: Accounts should not use trivial passwords. Passwords that meet the requirements in the SRS help prevent an attacker from gaining access to the system.

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. When the Account Policy window appears, verify that the "Minimum Password Length" is set to at least 8 characters. This setting will automatically disallow blank passwords.	The "Minimum Password Length" should be set to at least 8 characters.	Users should be trained to use alphanumeric and special characters in all passwords, use a minimum of one numeric character, do not use any word that can be found in a book or dictionary (forward or reversed), and do not use repeating characters in a password.	
2	Interview the administrator. Verify that the administrator account password is a password that meets the requirements in the SRS (i.e., in the expected results).	The "Administrator" account password is a password that meets SRS requirements (i.e., uses alphanumeric and special characters, uses a minimum of one numeric character, does not contain any word that can be found in a book or dictionary (forward or reversed), and does not contain repeating characters).	The "Administrator" account has virtually unlimited user rights and cannot be locked out, and so needs exceptionally careful protection from access by unauthorized users.	

Topic: I&A

Subtopic: Password Management

Test Objective 112 Verify that the default password expiration and minimum password length are set appropriately.

DII COE SRS Requirement: 3.2.1.4.2 Password life shall be limited to a maximum of 180 days. The COE shall notify the user prior to password expiration.

Rationale: Some systems allow the system administrator to set a "lifetime" for passwords. Users whose passwords are older than the time allowed are forced to change their passwords the next time they log in. If a user's password is exceptionally old, the system may prevent the user from logging in altogether.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. When the Account Policy window appears, verify that password age is set to 180 days.	In the Maximum Password Age list box the password age should be set to 180 days.	Regularly changing passwords limits the length of time a password obtained by an attacker can be used and limits the likelihood that a departed employee will still have access to the system. The tradeoff is that if the expiration time is set too short, users will either forget the new password, chose simple passwords or write it down.	
2	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. When the Account Policy window appears, verify that passwords cannot be reused until 10 other unique passwords intervene.	In the "Password Uniqueness" list box, 10 other unique passwords should be set.	This setting makes it more difficult for users to bypass the requirement to change passwords by immediately resetting the password to the original value.	
3	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu. When the Account Policy window appears, verify changing a password immediately after it is set is disallowed.	The "Minimum Password Age" is set to at least one day.	Makes it more difficult for users to bypass the no-reuse restriction.	

Topic: I&A

Subtopic: Mandatory profiles for shared user Ids

Test Objective 286 Verify that mandatory profiles are configured for shared UserIDs.

DII COE SRS Requirement: None Identified

Rationale: Shared UserIDs are a violation of security.

#	Required Action	Expected Results	Comments	Ö
1	Interview the System Administrator to determine if shared user Ids are being used, and if so, if mandatory profiles are being used.	Shared user Ids are NOT being used as this is a violation of User Identification and Authentication.	Do this if user IDs are used by several human users and the site is configured as a domain. Users with mandatory profiles cannot permanently change the desktop.	

Topic: I&A

Subtopic: Password Management

Test Objective 264 Verify that users are required to log on to change their passwords.

DII COE SRS Requirement: None Identified

Rationale: The effect of this setting is to prevent users from changing their own passwords after they expire; a system administrator must be involved. This limits the ability of an attacker to gain access to infrequently used/expired accounts.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then Account from the menu.	The "Users must log on in order to change password" item is checked off.		

Topic: I&A

Subtopic: User Accounts

Test Objective 266 Verify that the name of the administrator account has been changed from "Administrator" and is kept secret from non-privileged users.

DII COE SRS Requirement: None Identified

Rationale: The Administrator account has virtually unlimited user rights and cannot be locked out. Changing its name to one that is a closely held secret makes it more difficult for an attacker to determine the password.

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. The User Manager window appears.	Administrator does not appear in the Username list displayed.		
2	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\ SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software \Microsoft\Windows NT \CurrentVersion\Winlogon".	The "DontDisplayLastUserName" key is set to "1".	This protects the name of the administrator from being obtained.	
3	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT" directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click Default Computer. When the Default Computer Properties window appears, select Windows NT System, then Logon.	Check off "Do not display last logged on user name".	The previously logged on user name will not appear in the login dialog box.	

Topic: I&A

Subtopic: Accounts

Test Objective 103 Verify site identifying information is stored for all user accounts on the system.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, check the Description field for each user.	Each user's description field contains site identifying information.		

Topic: I&A

Subtopic: Accounts

Test Objective 102 Verify there are no guest accounts on the system.

DII COE SRS Requirement: None Identified

Rationale: Guest accounts present a security hole. By their nature, these accounts are rarely used, some are always used by people who should only have access to the machine for the short period of time that they are guests. The most secure way to handle guest accounts is to install them on an as-needed basis, and delete them as soon as the people using them leave. Guest accounts should never be given simple passwords such as "guest" or "visitor," and should never be allowed to remain in the password file when they are not being used (Curry, 1990).

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, double-click on the user "Guest".	The "Account Disabled" box IS checked in the "Guest" "User Properties" dialog box.	The "Guest" account is a known user ID on Windows NT systems and, as installed, does not require a password. "Guest" is a member of the group "Everyone" and has all the rig	

	window appears, select "Policies", "User Rights" from the menu. Select each right one at a time from the "Right" dropdown list and view the users granted the chosen right.		network and attack the Registry. Using these recommendations limits to some degree the damage that can be done if an attacker accesses the system as "Guest".	
3	Verify that any system on which the "Guest" account is enabled, with or without a password, is isolated as much as possible from the rest of the network and is not trusted by other systems on the network.	Any system on which the "Guest" account is enabled should not be part of a Windows NT domain, and should have unique user accounts.	Any system on which the "Guest" account is enabled is vulnerable to attacks on its Registry.	

Topic: Markings

Subtopic: Login Warning

Test Objective 6 Verify a security warning is displayed prior to the login process indicating restrictions that apply to logins, the highest classification of information processed on the system, and that misuse is subject to applicable penalties.

DII COE SRS Requirement: 3.2.7.1 The COE shall display a security warning prior to the login process that indicates the highest classification of information processed on the system and that misuse is subject to applicable penalties.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	View the monitor (screen) prior to login.	A security warning is displayed prior to the login process indicating restrictions that apply to logins, the highest classification of information processed on the system, and that misuse is subject to applicable penalties.		
2	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, click on the window "HKEY_LOCAL_MACHINE" and the folder "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon".	The "LegalNoticeCaption" and "LegalNoticeText" keys provide the required security warning.	The security warning is displayed upon each logon and the user is required to select the OK button in the warning dialog box before being able to proceed.	
3	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT" directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click Default Computer. When the Default Computer Properties window appears, select Windows NT User Profiles.	The "Delete cached copies of roaming profiles" is checked off.	This configuration will protect a user's profile by not making their profile available on a particular machine unless the user is currently logged on to it.	

Topic: Network Configuration

Subtopic: Anonymous FTP

Test Objective 134 Determine whether anonymous FTP is enabled on the system. If anonymous FTP is enabled, verify that it has been securely configured.

DII COE SRS Requirement: None Identified

Rationale: Anonymous FTP allows users who do not have an account on a machine to have restricted access in order to transfer from a specific directory. Because the anonymous FTP feature allows anyone to access the system (albeit in a very limited way), it should not be made available on every host on the network. If anonymous ftp is required, one machine should be chosen (preferably a server or standalone host) on which to allow this service. (Curry, 1990)

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, Microsoft Internet Server (Common), then Internet Service Manager. When the Microsoft Internet Service Manager window appears, double click the computer with the FTP service that requires configuration testing. Under the Service tab, verify that the "Allow Anonymous Connections" box is NOT checked. OR Attempt to login into the server using the user name "anonymous" and a valid mail name as the password.	The "Allow Anonymous Connections" box is NOT checked indicating that anonymous FTP is NOT enabled. OR The anonymous login attempt does NOT succeed.	This must be done if enabling the FTP server is required. Anonymous FTP connections break the trail of accountability from action to user.	
2	If the FTP server must be enabled, verify that a separate partition on an NTFS file system is the only partition to which read or write access is allowed via the FTP server. In the Taskbar, choose Start, Programs, Microsoft Internet Server (Common), then Internet Service Manager. When the Microsoft Internet Service Manager window appears, double click the computer with the FTP service that requires configuration testing. Under the Directories tab, verify that the Home Directory field contains the name of a separate NTFS partition.	The Directory listed in the Home Directory field contains the name of a separate NTFS partition that is ONLY used by the FTP server.	Windows NT 4.0 exports the entire partition containing the FTP home directory. Using a separate partition for the FTP server protects other files on the system from access via FTP.	
3	If anonymous FTP is enabled, verify	The Windows NT 4.0 FTP server has	The default FTP server that	

	that the Windows NT 4.0 FTP server has been replaced with another, more secure server.	been replaced with a more secure server.	ships with NT can poise security problems. Alternative more secure servers include: The SSL FTP Server. The Washington University (at St. Louis, MO) FTP Server. The problem is that you can set up your FTP site in c:\ftp, but when a user connects, they can then execute a "cd c:\winnt\system32", and be in your system directory (subject only to the ACLs that apply to the user name under which they connect).	
4	In the Taskbar, choose Start, Programs, Microsoft Internet Server (Common), then Internet Service Manager. When the Microsoft Internet Service Manager window appears, double click the computer with the FTP service that requires configuration testing. Under the Service tab, and in the Allow Anonymous Connections area, verify that the FTP user name is NOT "Guest" and that the account shown is not a member of any general user group.	The anonymous FTP user account is NOT "Guest".	This should be done if anonymous FTP is turned on. This configuration limits the damage that can be done by a user logging on as the ftp user.	
5	In the Taskbar, choose Start, Programs, Microsoft Internet Server (Common), then Internet Service Manager. When the Microsoft Internet Service Manager window appears, double click the computer with the FTP service that requires configuration testing. Under the Service tab, and in the Allow Anonymous Connections area, verify that the "Password" field contains a password.	The anonymous FTP user account has a password.	This should be done if anonymous FTP is turned on. This configuration prevents attackers from logging in directly using the anonymous FTP user account without requiring a password.	

Topic: Network Configuration

Subtopic: FTP

Test Objective 132 Determine whether FTP is enabled on the system. If FTP is enabled, verify that it has been securely configured.

DII COE SRS Requirement: None Identified

Rationale: The File Transfer Protocol (FTP) allows the user to transfer complete files between systems. There is both an ftp client program and an ftp server.

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	Attempt to connect to the local host using FTP.	If successful, then ftp is enabled. See configuration instructions for secure configuration.		
2	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Services icon. When the Services dialog box appears, find the FTP Publishing Service in the Service listbox.	If found, then ftp has been loaded into the system. See configuration instructions for secure configuration.		
3	To configure the FTP Server securely: After the FTP Server has been installed and you have restarted Control Panel, start the FTP Server option in Control Panel. Windows NT Server users can also use the FTP menu in Server Manager (located in the Program Manager icon, Administrative Tools group under the FTP pull down menu select FTP Server). The FTP User Sessions dialog box appears. Choose the Security button. The FTP Server Security dialog box appears. In the Partition box, select the drive letter you want to set security on, then check the "Allow Read" or "Allow Write" check box, or both check boxes, depending on the security you want for the selected partition. Repeat this step for each partition. Setting these permissions will affect all files across the entire FAT and HPFS partitions. On NTFS partitions, this feature can be used to remove read or write access (or both) on the entire partition. Choose the OK button when you are finished setting security access on partitions.	The FTP Server service is now ready to operate.	The changes take effect immediately. **Important: When you first install FTP Server, you must also configure FTP Server security so that users can access volumes on your computer.	

Topic: Network Configuration

Subtopic: Remote "r" Commands

Test Objective 88 Verify all "r" commands are disabled except for those specifically required.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\ SYSTEM32\" directory. Then delete all "r" commands found, such as the following: Rcp.exe Rsh.exe	Only those "r" commands which are specifically required are in the system.		

Topic: Network Configuration

Subtopic: Network Services

Test Objective 268 Verify that DHCP (Dynamic Host Configuration Protocol) has been deleted.

DII COE SRS Requirement: None Identified

Rationale: DHCP (Dynamic Host Configuration Protocol) dynamically reassigns IP addresses. Any security features that rely on IP addresses to identify hosts, such as some firewall systems, are less reliable if DHCP is used.

DHCP is not used for C2 configuration.

#	Required Action	Expected Results	Comments	Ö
1	From the Exploring window, select the "C:\WINNT\SYSTEM32" directory and determine if the "DHCP" directory exists.	The "DHCP" directory does not exist.		
2	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Services icon. When the Services dialog box appears, find all DHCP entries in the Services listbox.	All DHCP entries should be Disabled, or there should be none listed.	The system should not be using DHCP client, agent, and server services.	
3	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Network icon. When the Network dialog box appears, select the Services tab. In the Network Services list box, find all DHCP entries.	No DHCP entries should be found.	The system should not be using DHCP agent services.	

Topic: Network Configuration

Subtopic: Network Services

Test Objective 269 Verify that the Windows Internet Name Service (WINS) has been deleted.

DII COE SRS Requirement: None Identified

Rationale: WINS is not used in C2 configuration, and any unnecessary complexity of the operating system potentially increases vulnerability, therefore, this additional operating system capability should be removed.

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	From the Exploring window, select the "C:\WINNT\SYSTEM32" directory and determine if the "WINS" directory exists.	The "WINS" directory does not exist.	A WINS service does not exist.	
2	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Services icon. When the Services dialog box appears, find all WINS entries in the Services listbox.	All WINS entries should be Disabled, or there should be none listed.	The system should not be using WINS services.	
3	In the Taskbar, choose Start, Settings, then Control Panel. When the Control Panel window appears, double-click on the Network icon. When the Network dialog box appears, select the Services tab. In the Network Services list box, find all WINS entries.	No WINS entries should be found.	The system should not be using WINS services.	

Topic: System Architecture

Subtopic: Admin Tool Authorization

Test Objective 144 Verify that only authorized users are able to perform administrative tasks that can effect system security.

DII COE SRS Requirement: None Identified

Rationale: Many administrative tools can enhance the exploitation process if executed by someone who is trying to exploit the system.

#	Required Action	Expected Results	Comments	Ö
1	Verify that only users explicitly approved for performing backups, specifically excluding the Administrators group, have the right to backup files. In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, remove "Administrators" from and add either the group "Backup Operators" or specific users to the right "Backup files and directories".	In the "User Rights Policy" dialog box, "Administrators" has been removed from backup capabilities. The group "Backup Operators" or specific users have been added.	Use of the backup right grants access to all files, because a backed up file can be restored to a volume that does not have security enabled, such as a FAT file system, on any system, and use of this right bypasses all discretionary access control checks. Although Administrator can take ownership of any file and thereby gain access, the act of taking ownership is audited. Exercise of the backup right is not audited. Limiting the backup right to specific users increases the traceability of these file accesses.	
2	Verify that only users approved for performing restores have that right. In the Taskbar, choose Start, Programs, Administrative Tools, then User Manager or User Manager for Domains. When the User Manager window appears, select Policies, then User Rights from the menu. When the User Rights Policy window appears, remove "Administrators" from and add either the group "Backup Operators" or specific users to the right "Restore files and directories".	In the "User Rights Policy" dialog box, "Administrators" has been removed		

	directory. Double click on the "poledit.exe" file. When the System Policy Editor appears, double click the Default User, then System, finally Restrictions.			

Topic: System Architecture

Subtopic: Operating System

Test Objective 153 Verify the appropriate operating system patches have been applied.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Using telnet, ftp, or a network browser application, go to the following Microsoft site: //ftp.microsoft.com then to following folder/directory: /bussys/winnt/winnt-public/fixes /usa/nt40/ In NT40, go to the latest U.S. version Service Pack, such as ussp2. Look at the appropriate README files, then load the Service Pack for the correct hardware. If the node you are administering experiences a problem that is fixed by a hotfix, load that particular hotfix. Only load those hotfixes for which an actual problem exists on the node.	The latest Windows NT Service Pack and any required post-Service Pack hotfix should be installed.	Installing the latest Service Packs insures that the latest operating system bugs are corrected. Hotfixes should only be loaded to correct known problems.	

Topic: System Architecture

Subtopic: Printer Definition

Test Objective 154 Verify only appropriate printers are defined.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Settings, then Printers. When the Printers window appears, look at the list of printers.	Only the appropriate printers are defined in the list.		

Topic:	System Architecture
Subtopic:	Security Services
Test Objective 147	Verify the Security Services maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).
DII COE SRS Requirement:	3.2.14.1 The COE Security Services shall maintain a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures).
Rationale:	

#	Required Action	Expected Results	Comments	Ö
1	If the site has many Windows NT workstations, verify that if the site is configured as a domain, a primary domain controller and a backup domain controller are available.		This is recommended if the site has many Windows NT workstations. User account maintenance in a Workgroup configuration requires visiting each workstation, while user account maintenance in a Domain can be performed from a central location. Users can login into any Workstation in the Domain using a single userid and password and automatically have their own desktop environment available. In addition, the system hosting the SAM database can be protected more stringently than is convenient for user workstations.	

Topic: System Architecture

Subtopic: Security Support Tools

Test Objective 188 Verify security support tools are provided to periodically determine the security posture of systems, to validate the strength of the authentication mechanism, and to determine changes to designated systems and application files.

DII COE SRS Requirement: 3.2.15.6 The COE shall provide a standard set of security support tools to periodically determine the security posture of COE systems.
3.2.15.6.1 The COE shall provide the capability to validate the strength of the authentication mechanism. For example, the capability will check for potentially weak passwords.
3.2.15.6.2 The COE shall provide the capability to determine changes to designated systems and applications files, e.g., password or rc.* files.

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Verify that the System Administrator has access to the Windows NT 4.0 system documentation and to the Windows NT 4.0 Server and Workstation Resource Kits. Specifically, the C2 Security Configuration tool (c2config.exe) should be available.	The C2 Security Configuration tool is available.	Although administering a Windows NT system is much easier to administer than a UNIX system, it still requires some expertise. Unless it is maintained, the security configuration established at installation will degrade over time.	
2	Verify that a current virus protection program specific for Windows NT and capable of checking for macro viruses is available on the system.	A virus protection program is installed.	NOTE: Anti-virus programs need to be updated regularly. --------------------------- VirusScan for Windows NT McAfee Associates, Inc., 2710 Walsh Avenue, Santa Clara, CA 95051. Telephone: 408-988-3832 Fax: 408-970-9727 To Download McAfee Products BBS: 408-988-4004 (Settings: 8,N,1 Speed: Up to 28.8K) Internet FTP: ftp.mcafee.com WWW: http://www.mcafee.com CompuServe: GO	

			MCAFEE America Online: MCAFEE The Microsoft Network: MCAFEE NOTE: VirusScan for Windows NT 3.5.1 does not install on an NT Server! --------------------------- F-PROT Professional for Windows NT. Data Fellows Inc. 4000 Moorpark Avenue, Suite 207 San Jose, CA 95117 tel (408) 244 9090 fax (408) 244 9494 URL: http://www.datafellows.fi/f-prot/prodinfo/fp-nt.htm --------------------------- Norton Anti-virus for NT by Symantic, http://www.symantec.com/ --------------------------- While viruses specifically designed for Windows NT systems are not yet common, viruses are still a risk for Windows NT systems. Some MS-DOS viruses can do damage to a Windows NT system, and as Windows NT becomes more widespread, viruses designed for Windows NT will become more common.	
3	Verify that the tool DumpReg is available to the System Administrator.		DumpReg generates a report showing Registry key ACLs. DumpReg is available from "http://www.somarsoft.com."	
4	Verify that the tool DumpAcl is available to the System Administrator.		DumpAcl generates a report showing file ACLs. DumpAcl is available from "http://www.somarsoft.com."	

Topic: System Architecture

Subtopic: User Environment Configuration

Test Objective 158 Verify the user environment is configured properly.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, click on the window "HKEY_CLASSES_ROOT". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_CLASSES_ROOT" and all its subkeys are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read System - Full Control NOTE: The box "Replace Permissions on Existing Subkeys" is NOT checked.	These settings protect against an attacker changing the binding between file extensions and applications. Changing bindings could increase the risk of execution of Trojan Horse programs. The impact of these settings is that only members of the "Administrators" group may be able to install some software packages.	
2	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, bring up the window "HKEY_USERS" and the folder "HKEY_USERS\.DEFAULT\UNICODE Program Groups\". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_USERS\.DEFAULT\UNICODE Program Groups\[all subkeys]" are set to: Administrators - Full Control Everyone - Read System - Full Control	These settings protect the bindings between an icon and its program pathname. Changing the binding could increase risk of execution of Trojan Horse programs. The impact of these settings has not been fully investigated. Other trusted groups such as "Power Users" could be given "Full Control" access.	
3	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, bring up the window "HKEY_LOCAL_MACHINE". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\RPC\[all subkeys]" are set to: Administrators - Full Control SYSTEM - Full Control CREATOR OWNER - Full Control Everyone - ONLY Query Value, Enumerate Subkeys, Notify, and Read Control	The impact of leaving the default permissions for Everyone that allow Everyone to modify the RPC keys has not fully been analyzed; however, the suggested settings appear to provide useful protection without damaging functionality.	
4	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the	Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT		

	"\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, bring up the window "HKEY_LOCAL_MACHINE". Select "Security", then "Permissions" from the menu.	\CurrentVersion\[all subkeys] are set to: Everyone - ONLY Query Value, Enumerate Subkeys, Notify, Read Control		
5	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, bring up the window "HKEY_LOCAL_MACHINE". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Windows3.1MigrationsStatus\[all subkeys]" are set to: Everyone - Read.	This subtree contains Windows NT configuration information. This change may make it impossible for users not members of the Administrators group to install some software packages.	
6	In the Taskbar, choose Start, Programs, then select Explorer. When the Exploring window appears, select the "\<SYSTEMROOT>\WINNT\SYSTEM32" directory. Double click on the "Regedt32.exe" file. When the Registry Editor appears, bring up the window "HKEY_LOCAL_MACHINE". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Profile List are set to: Administrators - Full Control SYSTEM - Full Control CREATOR OWNER - Full Control Everyone - Special Access (Query Value, Create Subkey, Enumerate Subkeys, Notify, Read Control) (i.e., Turn off the Set Value permission.)	These settings allow caching of profiles while preventing an attacker from changing the filename pointing to a user’s profile. An untested enhancement would be to replace "Users" with the special group "INTERACTIVE". This would prevent an attacker from creating a Trojan key for a user who is not logged on.	

Topic: System Architecture

Subtopic: Operating System

Test Objective 152 Determine the OS version installed. Verify that it is the correct version.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	During installation, modify disk partitioning and formatting to remove any other operating systems.	Windows NT is the only operating system installed on the system.	If the system can be booted by MS-DOS, Windows 3.1 or 3.11, Windows 95 or LINUX, all Windows NT security features can be subverted. This includes the file system controls, since a program that runs under DOS that can access an NTFS file system is publicly available on the Internet. Omitting a second operating system from the hard drive does not provide complete protection, since it does not protect against booting from an MS-DOS floppy, but it is a desirable precaution.	
2	For existing systems, find out which version of the operating system is currently running on the node. In the Taskbar, choose Start, Programs, then Command Prompt. When the Command Prompt or MS-DOS Prompt window appears, type "ver" and press the Enter key.	The correct version of Windows NT is installed on the system.	If the system can be booted into a version of Windows NT that has not been configured as described in this document, some of the configured security features can be bypassed.	
3	Edit the boot.ini file as described in the Microsoft Windows NT Workstation Installation Guide, chapter 2, page 39.	Only the following two lines should be found in the boot.ini file under the caption "[operating systems]": multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server Version 4.00" multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server Version	The system should not have multi-boot capability from the same directory.	

		4.00 [VGA mode]" /basevideo /sos		
4	From the Exploring window, select the "C:\" partition and determine if any of the following directories exist: Windows Winnt32 Winnt	Only one such directory should exist on the C:\ boot partition.	The system should not have multi-boot capability from different directories.	
5	From the Exploring window, select the "D:\" partition and determine if any of the following directories exist: Windows Winnt32 Winnt Repeat the above procedure for any additional partitions found.	No such directory should exist on the D:\ boot partition.	The system should not have multi-boot capability from different partitions.	